150 Rose Orchard Way
San Jose, CA 95134
+1 408 576 1500

February 7, 2018

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

The Honorable Marsha Blackburn
Chairman
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

The Honorable Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

The Honorable Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Walden, Chairman Blackburn, Chairman Harper, and Chairman Latta:

Thank you for your letter dated January 24, 2018, requesting more information about Arm's response to recent findings about reported vulnerabilities, dubbed "Spectre" and "Meltdown." Arm appreciates the opportunity to respond to the Committee's questions and engage in dialogue on the coordinated vulnerability disclosure process.

There are three main variants of Spectre and Meltdown which, as noted in your letter, affect many modern processors. To date, we are not aware of any exploits or attempted exploits based on these vulnerabilities on affected Arm products.

The vast majority of chips based on Arm processors are **not impacted** by Meltdown or Spectre.[1] Nonetheless, Arm is taking this very seriously. Because Arm creates processor architectures that are licensed to semiconductor manufacturers, it does not have direct relationships with end users or most of the software providers in the supply chain. Therefore, our response and mitigation plans required a collaborative approach, including not only our customers but other software providers and industry.

For purposes relevant to this inquiry, Arm has two distinct types of commercial relationships with its direct licensees for processor technology:

- **"Implementation partners"** license processors that have been fully designed, developed, tested, and implemented by Arm itself. These partners then manufacture their own chips incorporating our technology.

- **"Architecture partners"** license Arm's processor architecture, and then design, develop, test and implement their own processors implementations based upon Arm's architectural definition. The architecture partners develop processors that, while software compatible, are proprietary in their implementation, and the specific detailed knowledge of the processors is not within Arm's knowledge or control. These partners then manufacture their own chips incorporating the Arm compatible processor that they have developed.

With respect to potential exploits, it is important to note that possible exploitations would be difficult, insofar as they appear to be dependent on malware running locally, which would have to be deployed on the target device. This means it is imperative for users to practice good security hygiene by keeping their software up-to-date and avoid suspicious links or downloads. Arm has emphasized this in the process of developing and promoting mitigations for Meltdown and Spectre.

1. Why was an information embargo related to the Meltdown and Spectre vulnerabilities imposed?

Information about the Meltdown and Spectre vulnerabilities was handled with discretion and care by Arm due to the potential risks of these vulnerabilities. As a general matter, Arm believes that vulnerability information is sensitive and should be treated with caution. Often, when vulnerabilities are discovered by security researchers, they will notify affected parties and provide time to develop solutions and mitigations before broader public disclosure. The length of time depends on the severity of a vulnerability, availability of a solution or mitigation, the complexity of developing such solutions, and potential impact of early disclosure.

Disclosures prior to ensuring effective mitigations are in place can be problematic. Information about vulnerabilities can assist bad actors in developing or attempting exploits. It can also unnecessarily alarm the public. "Responsible disclosure" or "coordinated disclosure" policies

[1] http://www.arm.com/security-update

are varied, subject to debate, and require careful coordination to maximize security and minimize unintended consequences.

Once informed about the possible vulnerabilities by Google Project Zero in June 2017, Arm placed a priority on evaluating the vulnerabilities, their potential impact on processors implemented by Arm, and developing mitigations and software that our architecture and implementation partners could use and deploy to secure their devices and operating systems. Within 10 days of learning of the potential exploits, Arm informed architecture partners to provide them knowledge so they could evaluate the vulnerabilities with respect to their own implementations of the Arm architecture. We informed our implementation partners and provided information regarding appropriate mitigations in January 2018.

2. What company or combination of companies proposed the embargo?

Many companies worked together and in parallel to respond in a timely manner to the issues identified by Google Project Zero. Arm worked with its licensees and coordinated with Google on issues relevant to Arm's handling of Spectre and Meltdown.

Google Project Zero proposed a public disclosure after a 90-day period.[2] It was agreed that this period should be extended. Arm believed that disclosure prior to having mitigations in place would have been premature and posed greater danger to the public. From the time of first learning of the potential exploits until present, Arm has worked to understand the possible threats and to provide mitigations for the affected Arm processors.

As Google Project Zero has publicly stated, public release of Spectre and Meltdown came before the "originally coordinated disclosure date of January 9, 2018" due to public speculation and discussion.[3]

3. When was the United States Computer Emergency Readiness Team (US-CERT) informed of the vulnerabilities?

Arm did not inform US-CERT of the vulnerabilities. Arm does not know if or when US-CERT was informed.

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) informed of the vulnerabilities?

Arm did not inform CERT/CC of the vulnerabilities. Arm does not know if or when CERT/CC was informed.

---

[2] https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html
[3] https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

5. Did your company perform any analyses to determine whether the embargo could have any negative impacts on critical infrastructure sectors such as healthcare and energy that rely on affected products? If so, what were the results? If no, why not?

Arm acted expeditiously to validate the issues and help its partners develop mitigations. Arm does not sell or license directly to users of chips that are based on Arm processors. Therefore, Arm is not in a position to communicate directly to healthcare or energy companies that rely on products that may contain chips that are built using Arm designs. However, Arm did seek to work with information technology companies that may serve such sectors.[4] Arm sought to expeditiously develop mitigations and then equip the companies within the industry with mitigations that could be applied by those companies to their products provided to end users.

As mentioned previously, information about vulnerabilities can assist bad actors in developing or attempting exploits. Therefore, Arm acted expeditiously to address the vulnerabilities, balancing speed of disclosure against preparedness for attempted exploits. In determining how to disseminate information about vulnerabilities and mitigations, Arm prioritized rapid development of technical solutions that could mitigate vulnerabilities and be used by its partners throughout the industry.

After the public disclosure, Arm communicated recommended mitigation measures to all impacted partners. The impact of this outreach and coordination was broad, covering licensees, developers, and users of Arm processors across a wide variety of business sectors and industries.

6. Did your company perform any analyses to determine whether the embargo could have any negative impacts on other information technology companies that rely on affected products? If so, what were the results? If no, why not?

As stated in the previous response, Arm is not in a position to communicate directly with all information technology companies that rely on products that may contain chips built using Arm processors. However, multiple companies within the supply chain, including major OS vendors, silicon suppliers, and other information technology vendors, were part of the group that Arm worked with, in respect of this issue. Our work with those companies indicated that Arm should expeditiously develop mitigations for these issues.

7. What resources or best practices did your company use in deciding to implement in the embargo?

Arm drew on its knowledge of the industry to most appropriately address the sharing and disclosure of information about Spectre and Meltdown to its customers. As previously stated in response to question 1, Arm believed that disclosures prior to ensuring effective mitigations are in place could be problematic. Arm worked with others in industry, such as OS vendors, to

[4] *See* Response to Question 6 for additional detail.

deploy such mitigations to ensure that bad actors were not assisted in developing or attempting exploits and that end users were not impacted by the risks presented by this issue.

8. What resources or best practices did your company use in implementing the embargo itself?

As expressed in previous responses, Arm worked collaboratively with its customers and others in industry to put appropriate mitigations in place to protect against the risks presented by this issue. Arm handled information about the Meltdown and Spectre vulnerabilities with discretion and care due to the potential risks of this vulnerability.

9. Based on your company's experience during this process, has your company established lessons learned relating to multi-party coordinated vulnerability disclosure? What are they?

Before Spectre and Meltdown, Arm had not been involved in multiparty coordinated vulnerability disclosure. Once Arm was notified by Google, this issue was made a major priority for the company. The issue received attention from senior leadership, key engineers, and our Board of Directors was made aware. We are confident Arm acted with the appropriate urgency, dedicating substantial resources to Spectre and Meltdown and assisting the entire industry to identify and respond to these vulnerabilities.

Based on this experience we are evaluating what lessons can be learned and used for future process improvements. In particular, we are reviewing the method by which external parties notify Arm of vulnerabilities, adopting a formal vulnerability disclosure process, and determining how best to notify appropriate entities while avoiding inadvertent public disclosure prior to appropriate mitigations.

If you have any additional questions, please do not hesitate to contact me or Vince Jesaitis, Arm's Director of Government Affairs, at 1-202-718-6272.

Yours sincerely,

Simon Segars, CEO

cc:
Congressman Frank Pallone, Ranking Member, House Committee on Energy and Commerce
Congressman Mike Doyle, Ranking Member, House Subcommittee on Communications and Technology
Congresswoman Diane DeGette, Ranking Member, House Subcommittee on Oversight and Investigations
Congresswoman Jan Schakowsky, Ranking Member, House Subcommittee on Digital Commerce and Consumer Protection